Department of the Interior
Privacy Impact Assessment

September 8, 2014

Name of Project: Enterprise Forms System
Bureau: Office of the Secretary
Project's Unique ID (Exhibit 300): 010-000000312

Once the PIA is completed and the signature approval page is signed, please provide copies of the PIA to the following:

- Bureau/office IT Security Manager
- Bureau/office Privacy Act Officer
- DOI OCIO IT Portfolio Division
- DOI Privacy Act Officer

Do not email the approved PIA directly to the Office of Management and Budget email address identified on the Exhibit 300 form. One transmission will be sent by the OCIO Portfolio Management Division.

Also refer to the signature approval page at the end of this document.

A. CONTACT INFORMATION:

Teri Barnett
Departmental Privacy Officer
Office of the Chief Information Officer
U.S. Department of the Interior
1849 C Street NW, Mail Stop 5547 MIB
Washington, DC 20240
Phone: (202) 208-1605

B. SYSTEM APPLICATION/GENERAL INFORMATION:

1) **Does this system contain any information about individuals?**

   a. **Is this information identifiable to the individual[1]?** (If there is NO information collected, maintained, or used that is identifiable to the individual in the system,

[1] "Identifiable Form" - According to the OMB Memo M-03-22, this means information in an IT system or online collection: (i) that directly identifies an individual (e.g., name, address, social security number or other identifying number or code, telephone number, email address, etc.) or (ii) by which an agency intends to identify specific

Sections D through G can be marked not applicable. If YES complete all sections for system and any applicable minor applications).

Yes, the Enterprise Forms System (EFS) contains personally identifiable information (PII) about current and former DOI employees, contractors and volunteers, other Federal, state, territorial or local government employees, contractors and volunteers, individuals from Indian tribes, vendors, partners, business owners, entrepreneurs, procurement officials, investors, lawful permanent residents, members of the public in the U.S. States, territories, and U.S. Insular Areas, foreign nationals, and other individuals who may wish to interact with the Department of the Interior (DOI or Department) by using the EFS to access, complete, and submit forms.

b. **Is the information about individual members of the public?** (If YES, a PIA must be submitted with the OMB Exhibit 300, and with the IT Security C&A documentation).

Yes. The system contains PII on individual members of the public who may wish to interact with the Department by using the EFS to access, complete, and submit forms.

c. **Is the information about employees?** (If yes and there is no information about members of the public, the PIA is required for the DOI IT Security C&A process, but is not required to be submitted with the OMB Exhibit 300 documentation).

Yes. The system contains PII about current and former DOI employees, contractors and volunteers who may use the EFS to access, complete, and submit forms, as well as employees who process forms.

2) **What is the purpose of the system/application?**

The EFS is a component of the eMail Electronic Records and Document Management System (eERDMS), which is a major application program that supports the EFS as well as the Enterprise eArchive System (EES), Enterprise Content System (ECS), and Enterprise Dashboard System (EDS). These components provide the framework for storing, accessing, and managing the Department's records, and for preventing the loss of records that should be kept for legal and accountability purposes. Due to the complexity of these systems, privacy impact assessments were conducted separately for the eERDMS, EES, ECS, and EDS, which may be viewed at http://www.doi.gov/ocio/information_assurance/privacy/ppia.cfm.

The EFS will consolidate all internal forms used by the Department and external forms used by the public into a centralized automated forms program. This will increase efficiency and responsiveness through the centralization and automation of all Department forms, as well as creating the ability to view business trend analysis and

individuals in conjunction with other data elements, i.e., indirect identification. (These data elements may include a combination of gender, race, birth date, geographic indicator, and other descriptors).

processing metrics. In addition, the forms process will be modernized through the implementation of a completely digital workflow, the integration of digital and electronic signatures, and the ability to utilize real-time workflow through the use of unified messaging.

Each form will be added to the EFS under the direction of a Form Manager, who will typically be a representative of the DOI Bureau or Office that owns the form. The Form Manager will oversee and direct the conversion of the form, including the setup of the form and various data entry controls, along with parameters for data expiration. Once a form has been added to the EFS, a Form Owner will monitor form submissions, including reviewing data and correcting submissions or contacting form submitters for additional or corrected information, as necessary. Similar to the Form Manager, the Form Owner will also typically be a representative of the DOI Bureau or Office that owns the form.

3) What legal authority authorizes the purchase or development of this system/application?

Departmental Regulations, 5 USC 301; The Paperwork Reduction Act, 44 U.S.C. Chapter 35; the Clinger-Cohen Act, 40 U.S.C. 1401; OMB Circular A-130, Management of Federal Information Resources; Executive Order 13571, “Streamlining Service Delivery and Improving Customer Service”, April 11, 2011; Presidential Memorandum, “Security Authorization of Information Systems in Cloud Computing Environments”, December 8, 2011; Presidential Memorandum, “Building a 21st Century Digital Government”, May 23, 2012.

C. <u>DATA IN THE SYSTEM:</u>

1) What categories of individuals are covered in the system?

The individuals covered in the EFS include current and former DOI employees, contractors and volunteers, other Federal, state, territorial or local government employees, contractors and volunteers, individuals from Indian tribes, vendors, partners, business owners, entrepreneurs, procurement officials, investors, lawful permanent residents, members of the public in the U.S. States, territories, and U.S. Insular Areas, foreign nationals, and other individuals who may wish to interact with the Department by using the EFS to access, complete, and submit forms.

2) What are the sources of the information in the system?

a. Is the source of the information from the individual or is it taken from another source? If not directly from the individual, then what other source?

Sources of the information are from members of the general public; individuals from Indian tribes; DOI employees, contractors, and volunteers; other Federal, state, territorial and local government officials, contractors and volunteers; non-governmental organizations; and other individuals who wish to interact with DOI by utilizing the EFS to access, complete, or submit forms. In some instances, such as with specific types of human resources forms, DOI employees acting within the scope of their job duties may submit individual personal information on behalf of others using standardized forms. In addition, the system may apply Active Directory Federated Service (ADFS) queries to look up and auto fill contact information for Federal employees using the system.

b. What Federal agencies are providing data for use in the system?

Certain forms will be submitted by officials, employees, or representatives of other Federal agencies where DOI is partnering or engaging with those agencies on specific program initiatives or activities or where the Federal agencies are requesting information or services from DOI. The data provided will vary based on the subject matter of the form. Some data pertaining to individuals may be included in these submissions, such as personal information included on incident reports involving accidents or crimes on DOI lands that involve response efforts from numerous Federal agencies. Otherwise, it is not currently anticipated that other Federal agencies will be providing significant amounts of individual information.

c. What Tribal, State and local agencies are providing data for use in the system?

Certain forms will be submitted by officials, employees, or representatives of various Tribal, State and local agencies where DOI is partnering or engaging with those agencies on specific program initiatives or activities or where the agencies are requesting information or services from DOI. The data provided will vary based on the subject matter of the form. Some data pertaining to individuals may be included in these submissions, such as personal information included on incident reports involving accidents or crimes on DOI lands that involve response efforts coordinated with Tribal, State or local agencies. Otherwise, it is not currently anticipated that other agencies will be providing significant amounts of individual information.

d. From what other third party sources will data be collected?

Data will be collected using forms in the EFS from various third parties that have business relationships or partnerships with DOI, including contractors, vendors, and lessors.

e. What information will be collected from the employee and the public?

This system contains large amounts of information including, but not limited to: name, username, Social Security number, email address, home or work address, phone number, other contact information, gender, age, date of birth, nationality, country of origin, country of citizenship, citizenship status, passport number, driver's license information, Tribal enrollment number, Indian tribal information, Federal, state or local government agency identification number, vehicle registration information, information about personal characteristics such as height, weight, race, employment status, employment background and related information, eligibility determinations, IP address, credit card number, bank account information, other financial information, medical information, information concerning disabilities, criminal background information, security clearance, education information, and information regarding certifications and licenses. The system may also include other categories of information obtained from official forms submitted to and processed by DOI.

3) Accuracy, Timeliness, and Reliability

a. How will data collected from sources other than DOI records be verified for accuracy?

Individuals submitting forms to DOI will be responsible for the accuracy of the data provided. In addition, each Form Manager will design their form in a manner that encourages the submission of accurate information. The design process will include process diagramming, including the creation of swim lane process maps. Among other benefits, these process maps will limit data entry options as a user moves through a form to ensure consistency with data entered in earlier fields on the form. In addition, forms will include data integrity validation controls where appropriate, such as drop down menus, check boxes, text field size limitations, and predefined numeric formats.

Form submissions will be reviewed by the responsible Form Owner, who will be notified upon each new form submission. The Form Owner will have the opportunity to review the form and either correct inaccurate data or contact the submitter of the form to request corrections. The system contains an audit function that allows system administrators to check forms review status by running reports on specific Form Owners, and escalating reviews as necessary.

b. How will data be checked for completeness?

Individuals submitting forms to DOI will be responsible for the completeness of the data provided. In addition, each Form Manager will design their form in a manner that enforces the submission of complete information. The design process will include process diagramming, including the creation of swim lane process maps. Among other benefits, these process maps will limit data entry options as a user moves through a form to ensure additional data is entered when follow up information is necessitated by prior form entries. In addition, forms will include data integrity validation controls where appropriate, such as drop down menus, check boxes, text field size limitations, and predefined numeric formats.

Form submissions will be reviewed by the responsible Form Owner, who will be notified upon each new form submission. The Form Owner will have the opportunity to review the form and either correct inaccurate data or contact the submitter of the form to request corrections or additional information. The system contains an audit function that allows system administrators to check forms review status by running reports on specific Form Owners, and escalating reviews as necessary.

c. Is the data current? What steps or procedures are taken to ensure the data is current and not out-of-date? Name the document (e.g., data models).

By default, data will have a life cycle of twelve months. Form Managers can shorten or lengthen the data life cycle, based upon the nature of the data at issue, retention schedules, or other factors. When data reaches expiration, the Form Owner will receive notification, and will have the option to allow the data to expire or can contact the submitter to request updated information.

The use of ADFS queries, as noted above in section C(2)(a), will result in automatic updates of DOI employee contact information in EFS when the contact information is updated in the active employee directory, thereby maintaining currency of the information.

d. Are the data elements described in detail and documented? If yes, what is the name of the document?

The data elements are generally described in the EFS IT Security Assessment and Authorization (A&A) documentation.

The EFS will ultimately contain thousands of forms, and will continue to expand as new forms are developed. While many of the forms will have common data element types, such as names, addresses, and telephone numbers, many additional and unique data fields may be incorporated, depending on the content of specific forms. Therefore, there is not a single document (or documents) that list all of the specific data types included in the EFS.

However, the EFS has been designed to comply with several important standards in order to ensure consistency, information operability and precise descriptions of data. First, the EFS utilizes the World Wide Web Consortium (W3C) Extensible Markup Language (XML), which provides a means for consistent and common data naming conventions.

In addition, the EFS is National Information Exchange Model (NIEM) compliant. NIEM is an XML-based information exchange framework that was designed collaboratively by the Department of Justice and the Department of Homeland Security as a means to develop, disseminate, and support enterprise-wide information exchange standards and processes.

The use of these standards in the EFS will not only improve development and facilitate a more organized collection of data, but also may result in a reduction in the total amount of data that the system collects, as well as promoting proper data protection, maintenance, and retention practices.

D. ATTRIBUTES OF THE DATA:

1) Is the use of the data both relevant and necessary to the purpose for which the system is being designed?

Yes. The EFS system consolidates existing Departmental and DOI Bureau and Office forms, and the processing of each form requires the collection and use of specific data. For all forms added to the EFS, the individual Form Manager is responsible for limiting information collection in accordance with all applicable laws, regulations, and DOI policies, and for ensuring that the data collected is both relevant and necessary.

2) Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected, and how will this be maintained and filed?

No, the system will not derive new data or create previously unavailable data. While new data could potentially be derived or created by aggregating or utilizing information provided by individuals who have submitted multiple forms in the EFS, the EFS is not intended to be used in that manner. The ability to derive new data is limited by the design of the EFS, which restricts Form Owners' access to the data obtained from the forms they manage.

3) Will the new data be placed in the individual's record?

The system will not derive new data or create previously unavailable data. As discussed above, the EFS is not intended to be used to derive new data about individuals, therefore, no new data will be placed in individuals' records. If future use of the EFS changes to include the creation and use of new data, an amendment to this PIA will be issued, which will discuss the new data to be created and any placement in records of individuals.

4) Can the system make determinations about employees/public that would not be possible without the new data?

No, the system will not derive new data or create previously unavailable data. While new data could potentially be derived or created by aggregating or utilizing information provided by individuals in the course of submitting multiple different forms, the EFS is not intended to be used in that manner. As with many automated information systems, the data in the EFS could be combined or aggregated to make determinations about individuals that would not otherwise be possible. However, the ability to derive new data is limited by the design of the EFS, which restricts Form Owners' access to the data obtained from the forms they manage. If future use of the EFS changes to include the creation and use of new data, an amendment to this PIA will be issued which will describe the new data to be created and the determinations that might be made about employees or members of the public using the new data.

5) How will the new data be verified for relevance and accuracy?

The system will not derive new data or create previously unavailable data. While new data could potentially be derived or created by aggregating or utilizing information provided by individuals in the course of submitting multiple different forms, the EFS is not intended to be used in that manner. If future use of the EFS changes to include the creation and use of new data, an amendment to this PIA will be issued which will outline procedures for verifying the relevance and accuracy of the new data.

6) If the data is being consolidated, what controls are in place to protect the data from unauthorized access or use?

The EFS will centralize and consolidate the storage and management of all DOI Departmental, Bureau, and Office forms into a single forms repository. While all of the data in the EFS will be stored in a common database, the data will be separated by limiting Form Owners' access to the data obtained from the forms they manage.

System access is granted to authorized personnel on an official need to know basis. Unique user identification and authentication, passwords, least privileges and audit logs are utilized to ensure appropriate permissions and access levels. All personnel must consent to rules of behavior and complete annual security, privacy and records management training. Form Managers will only have access to the data submitted for the forms they manage. Individual end users of the system will have access only to information that they have personally submitted.

7) If processes are being consolidated, are the proper controls remaining in place to protect the data and prevent unauthorized access? Explain.

The EFS will centralize and consolidate the storage and management of all DOI Departmental, Bureau, and Office forms into a single forms repository. While the forms management process is being consolidated, the ownership of the data obtained from the forms will remain with the Bureau or Office generating the form, and each form will have a designated Form Owner to manage form submissions.

System access is granted only to authorized personnel on an official need to know basis. Unique user identification and authentication, passwords, least privileges and audit logs are utilized to ensure appropriate permissions and access levels. All personnel must consent to rules of behavior and complete annual security, privacy and records management training. Form Managers will only have access to the data submitted via the forms they manage. Individual end users of the system will have access only to information that they have personally submitted.

8) How will the data be retrieved? Does a personal identifier retrieve the data? If yes, explain and list the identifiers that will be used to retrieve information on the individual.

Data can be retrieved in the EFS by Form Owners or System Administrators using any word or part of a word or number (a keyword search), including personal identifiers or parts of personal identifiers, such as names, Social Security numbers, email addresses, home or work addresses, usernames, assigned matter numbers, and subject matter index. Individuals who have submitted forms can access only their own data, and can do so using a login and password that is established when they initially register and create a user account to use the EFS system.

9) What kinds of reports can be produced on individuals? What will be the use of these reports? Who will have access to them?

The system will not generate reports on individual users of the system. The EFS auditing system allows reports to be generated on various aspects of the system's operating controls, including system functions and user actions. The EFS contains an auditing function that tracks all actions by users of the system, including username, date and time of access, and attempts to access unauthorized information. In general, reports about individuals will not be produced. However, reports will be produced to identify the status of form submission reviews by the Form Owners. These reports will be utilized to ensure that forms reviews are being performed in a timely manner, and to facilitate the escalation of forms reviews if necessary.

10) What opportunities do individuals have to decline to provide information (i.e., where providing information is voluntary) or to consent to particular uses of the information (other than required or authorized uses), and how individuals can grant consent.)

Individual opportunity to consent to or decline the collection or provision of personal information occurs at the time an individual submits a form. Pursuant to the Privacy Act and Departmental policy, any form that collects PII that is maintained in a system of records must include a Privacy Act Statement advising individuals of the authority for the information being collected, the purpose and uses of the information, any impact to the individual for not providing the requested information. Certain form fields may be optional, while other form fields are mandatory, and the submission of a form is a voluntary act by the submitter. The impact to the individual for not completing a form varies with each form, and in some cases failure to complete a form may hinder requests for DOI services.

As with all DOI websites, the EFS is subject to DOI's website Privacy Policy (http://www.doi.gov/privacy.cfm). As noted in the Privacy Policy, DOI collects information such as IP address and date and time of visit. This information is not stored in the EFS, but is retained in log files held by DOI's Enterprise Services Network. This information is not held with other PII such as names or email addresses. Users can prevent the collection of this information by not using DOI websites, or through the use of services or settings that anonymize web browsing.

E. MAINTENANCE AND ADMINISTRATIVE CONTROLS:

1) If the system is operated in more than one site, how will consistent use of the system and data be maintained in all sites?

The primary system is being maintained at a single site, which will be mirrored to a secondary site for backup purposes or to provide coverage in the event of a significant outage of the primary system. Absent a significant outage, all data transfer will be unidirectional from the primary server to the backup server. No additional data collection will occur on the backup server. As a result, the data in each location will be consistent. In the event that the backup server is used to run the system during an extended outage period, specific automated controls are in place to ensure the complete transfer of all collected data back to the primary server.

2) What are the retention periods of data in this system?

Records contained within the EFS are retained and disposed of in accordance with applicable Departmental, Bureau, or Office records schedules, or General Records Schedule (GRS) approved by the National Archives and Records Administration (NARA) for each type of record or form based on the subject matter and records series.

3) What are the procedures for disposition of the data at the end of the retention period? How long will the reports produced be kept? Where are the procedures documented?

Records are disposed of in accordance with the applicable Departmental, Bureau, or Office records retention schedules and Departmental policy. Paper records are disposed of by shredding or pulping, and records contained on electronic media are degaussed or erased in accordance with 384 Departmental Manual 1 and NARA guidelines.

4) Is the system using technologies in ways that the DOI has not previously employed (e.g., monitoring software, Smart Cards, Caller-ID)?

Yes. EFS is the first Department-wide cloud based enterprise forms system implemented at DOI. In addition, the creation of a single enterprise-wide web-based system to electronically collect, store and maintain all of DOI's forms represents a significant technological shift.

5) How does the use of this technology affect public/employee privacy?

Cloud Storage:

The EFS maintains forms submitted by individuals that may contain PII, which presents privacy risks for members of the public and employees. The EFS will be hosted by a Federal Information Security Management Act (FISMA) moderate compliant cloud services vendor. The evaluation of cloud-based hosting services became mandatory upon the release of the "Federal Cloud Computing Strategy" by the White House in February, 2011. Since that time, security concerns have been evaluated, and security protocols and procedures for federal cloud applications have been put forth by the National Institute of Standards and Technology (NIST). The EFS will be hosted by a cloud provider that complies with all NIST standards.

Enterprise-wide Web-Based Electronic Forms System:

The EFS will consolidate the collection, storage and management of all DOI Departmental, Bureau, and Office forms into a single forms repository. While all of the data in the EFS will be stored in a common database, the data will separated by limiting access to authorized Form Owners who will have access only to the data contained on the forms they manage. As a result, the creation of a common system for all of DOI's forms should not result in enhanced privacy risks. Moreover, the use of a single system will permit all form data collected by DOI to be held and maintained with consistent security, privacy, and records management standards and practices.

6) Will this system provide the capability to identify, locate, and monitor individuals? If yes, explain.

The EFS generally will not have the potential to identify, locate and monitor individuals, though the system will have the ability to audit usage of the system, including use by system administrators, Form Managers, and Form Owners. This includes reviewable data concerning logins, including login date and time. In addition, the system will monitor workflow, including monitoring the status of reviews of new forms by Form Owners. In the event that review of system workflows reveals that reviews are not being performed in a timely fashion, the matter will be escalated.

7) What kinds of information are collected as a function of the monitoring of individuals?

The system is not intended to monitor individuals, though the system will have the ability to audit usage of the system, including use by system administrators, Form Managers, and Form Owners. This includes reviewable data concerning logins, including login date and time. In addition, the system will monitor workflow, including monitoring the status of reviews of new forms by Form Owners. In the event that review of system workflows reveals that reviews are not being performed in a timely fashion, the matter will be escalated.

8) What controls will be used to prevent unauthorized monitoring?

The system is not intended to monitor individuals. However, the system will have the ability to audit usage of the system, including use by system administrators, Form Managers, and Form Owners. This includes reviewable data concerning logins, including login date and time. In addition, audit logs, access level restrictions, and least privileges are used to ensure users have access only to the data they are authorized to view, which serves as a control on unauthorized monitoring. Also, firewalls and network security arrangements are built into the architecture of the system and NIST guidelines and Departmental policies are fully implemented. System administrators will review the use of the EFS and the activities of users to ensure that the system is not improperly used, and to prevent unauthorized monitoring or access.

9) Under which Privacy Act systems of records notice does the system operate? Provide number and name.

Not applicable. The DOI Office of the Solicitor has determined that the EFS is not a Privacy Act system of records, and therefore a Privacy Act system of records notice is not required to be published in the Federal Register. There are numerous forms within the EFS that fall under other published government-wide, Department-wide, Bureau, or Office Privacy Act system of records notices. Individuals must review the applicable system of records notice for each form submitted for specific information pertinent to the collection and maintenance of information. DOI Privacy Act system of records notices may be viewed at http://www.doi.gov/ocio/information_assurance/privacy/privacy-act-notices-9-06-06.cfm.

10) If the system is being modified, will the Privacy Act system of records notice require amendment or revision?

Not applicable. The DOI Office of the Solicitor has determined that the EFS is not a Privacy Act system of records, and therefore a Privacy Act system of records notice is not required to be published in the Federal Register. There are numerous forms within the EFS that fall under other published government-wide, Department-wide, Bureau, or Office Privacy Act system of records notices. Any amendment or revision to these notices is the responsibility of the Privacy Act system manager for each system as appropriate. Individuals must review the applicable system of records notice for each form submitted for specific information pertinent to the collection and maintenance of information. DOI Privacy Act system of records notices may be viewed at http://www.doi.gov/ocio/information_assurance/privacy/privacy-act-notices-9-06-06.cfm.

F. ACCESS TO DATA:

1) Who will have access to the data in the system? (e.g., contractors, users, managers, system administrators, developers, tribes, other)

Authorized DOI Form Managers, system administrators, and authorized users will have access to the data in EFS. Access to information will be limited to those personnel that have a need to know the data in order to perform official duties. Individuals who submit forms will have access only to the forms and data they submit. Form Managers will have access only to the data obtained through the forms they manage. Access to the EFS by system administrators, authorized program personnel, and contractors is based on least privileges.

2) How is access to the data by a user determined? Are criteria, procedures, controls, and responsibilities regarding access documented?

Access level restrictions, authentication, least privileges, and audit logs are used to ensure users have access only to the data they are authorized to view. Form Managers' access to the data is limited to those who have official forms management responsibilities. Access is further governed by DOI IT security policy, including use of assigned passwords, limited access rules, various firewalls, and other protections put in place to assure the integrity and protection of any personal information. All DOI employees and contractor employees undergo initial and annual Security Awareness, Privacy and Records Management training, and sign rules of behavior agreeing to comply with DOI policies and protect personal information before being granted access to DOI networks and information.

3) Will users have access to all data on the system or will the user's access be restricted? Explain.

Individuals that submit forms will have access only to their own data. Each form has a designated Form Manager that has access to all information submitted via the form they manage. System administrators have access to audit reports on various aspects of the system's operating controls, including system functions and user actions.

Computer records are protected by a password system that is compliant with NIST standards as specified in NIST Special Publication (SP) 800-53 Rev. 4, "Security and Privacy Controls for Federal Information Systems and Organizations," and NIST SP 800-37, "Guide for Applying the Risk Management Framework to Federal Information Systems." The records contained in this system are safeguarded in accordance with applicable security rules and policies. Access to servers containing records in this system is limited to authorized personnel who have a need to know the information for the performance of their official duties and requires a valid username and password. Unique user identification and authentication, such as passwords, least privileges and audit logs are utilized to ensure appropriate permissions and access levels.

4) What controls are in place to prevent the misuse (e.g., unauthorized browsing) of data by those having access? (Please list processes and training materials)

Audit logs, access level restrictions, and least privileges are used to ensure users have access only to the data they are authorized to view. In addition, firewalls and network security arrangements are built into the architecture of the system and NIST guidelines and Departmental policies are fully implemented. System administrators will monitor the use of the EFS and the activities of the users to ensure that the system is properly used.

The EFS has multiple layers of security that protect content to the object level and can be applied to a user, group of users, or set as a general feature. Account access within the EFS is also limited to defined time periods; after a certain period of inactivity user accounts will be logged out of the system. The EFS can generate both usage and access reports that can be monitored by system administrators.

Additionally, the EFS contains a user traceability program that can detect unauthorized access attempts or access to files outside of their permissions. The audit trail feature, unique identification, authentication and password requirements, and mandatory security, privacy and records management training requirement prevent unauthorized access to data, browsing and misuse.

5) Are contractors involved with the design and development of the system and will they be involved with the maintenance of the system? If yes, were Privacy Act contract clauses inserted in their contracts and other regulatory measures addressed?

Contractors are involved in the design and development of the system and Privacy Act clauses were inserted in their contracts.

6) Do other systems share data or have access to the data in the system? If yes, explain.

The EFS currently uses ADFS queries to look up and auto fill contact information for Federal employees, but does not interface or share information with other systems at this time. However, in the future DOI anticipates using the EFS to interact with other internal systems to facilitate the business management process.

The EFS is a component of eERDMS, a major application program that also hosts the EES, ECS, and EDS components. These components provide the framework for storing, accessing, and managing the Department's records, and for preventing the loss of records that should be kept for legal and accountability purposes. The EFS consolidates all internal and external forms into a centralized automated forms program, and creates the ability to view business processes, utilize real-time workflow, and facilitate forms management. As part of this business process, records or data in the EFS may be shared or stored in the other eERDMS components. Due to the complexity of these components, privacy impact assessments were conducted separately for the eERDMS, EES, ECS, and EDS, which may be viewed at http://www.doi.gov/ocio/information_assurance/privacy/ppia.cfm.

7) **Who will be responsible for protecting the privacy rights of the public and employees affected by the interface?**

The system manager, security manager and system administrator for the EFS will have the responsibility for protecting the privacy rights of the public and employees.

8) **Will other agencies share data or have access to the data in this system (Federal, State, Local, Other (e.g., Tribal))?**

No, the EFS will not share data or provide access to data to other Federal agencies.

9) **How will the data be used by the other agency?**

Not applicable – other agencies will not have access to or share data in the system.

10) **Who is responsible for assuring proper use of the data?**

The system owner, system manager, security manager and system administrator for the EFS will have the responsibility for ensuring the proper use of the data.